(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
25 January 2001 (25.01.2001)

PCT

(10) International Publication Number
WO 01/06468 A1

(51) International Patent Classification[7]: G07F 7/10, G06F 19/00

(21) International Application Number: PCT/US00/19706

(22) International Filing Date: 19 July 2000 (19.07.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/144,503 19 July 1999 (19.07.1999) US
09/618,691 18 July 2000 (18.07.2000) US

(71) Applicant: DATACARD CORPORATION [US/US]; 11111 Bren Road West, P.O. Box 9355, Minneapolis, MN 55440 (US).

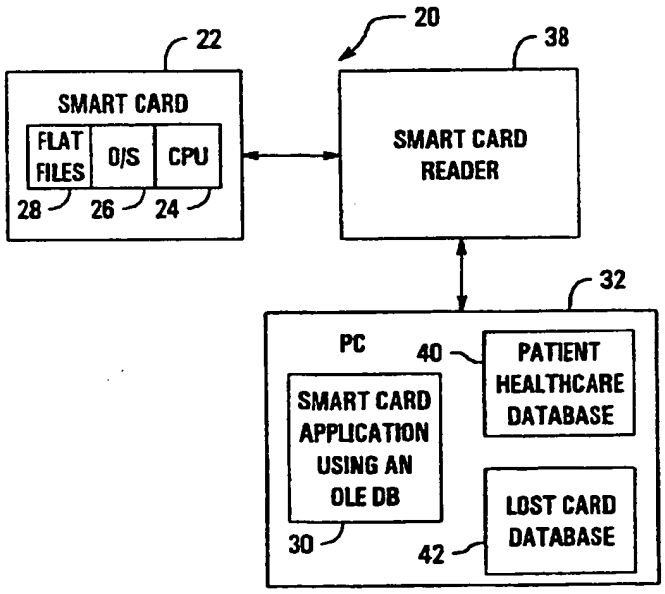
(72) Inventors: NELSON, David; 17281 - 88th Avenue North, Maple Grove, MN 55369 (US). HENKEL, Scott; 8592 Ridge Ponds Drive, Victoria, MN 55386 (US). WARTHEN, Michael; 22 Greenspring, Dove Canyon, CA 92679 (US). SHARMA, Ravi; 17 Augusta, Coto De Cava, CA 92679 (US). ERICKSON, Hans; 4325 Medray Avenue, Eagan, MN 55122 (US). MILLER, Scott, D.; 1366 Carriage Road, Woodbury, MN 55125 (US). MILLER, Charlotte, M.; 12528 Pineburst, Burnsville, MN 55337 (US). BERGSTROM, Andrew, W.; 5629 James Avenue South, Minneapolis, MN 55419 (US). VANWAGNER, Lee, O.; 5231 Surf Drive, Rockford, MI 49341 (US). HENNINGER, Jeff, L.; 3700 Monaltrie Avenue, Deephaven, MN 55391 (US). FRAZER, Anne, L.; 7349 Inman Avenue South, Cottage Grove, MN 55016 (US).

(74) Agent: BRUESS, Steven, C.; Merchant & Gould P.C., P.O. Box 2903, Minneapolis, MN 55402-0903 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AT (utility model), AU, AZ, BA, BB, BG, BR, BY, BZ, CA,

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR STORING, MANAGING, AND RETRIEVING HEALTHCARE INFORMATION ON A SMART CARD



(57) Abstract: A patient healthcare record system for storing, managing, and retrieving healthcare information via a smart card includes the smart card having a processor, an operating system, and at least one file; a smart card reader operable to read/write the smart card; and a PC, a server PC, or an Internet web portal/server coupled to the smart card reader directly, via a client PC, or via a web browser device. The system also includes a smart card application having a database interface operable to convert the at least one file stored on the smart card to a smart card database file. Further, the system includes a system database file that includes patients' healthcare information. The smart card database file is a subset of the system database file. The smart card database file is capable of being read/written, and may contain a security code to access the system database file. The methods for storing, managing, and retrieving healthcare information via a smart card include a method of issuing a new smart card, a method of accessing and updating a return patient's smart card by a care provider, a method of accessing and updating a referral patient's smart card by a care provider, a method of accessing and updating a patient's smart card by an authorized paramedic/emergency team, a method of accessing and updating a patient's smart card by a patient; and a method of accessing a lost card database and issuing a new smart card.

WO 01/06468 A1

CH, CN, CR, CU, CZ, CZ (utility model), DE, DE (utility model), DK, DK (utility model), DM, DZ, EE, EE (utility model), ES, FI, FI (utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KR (utility model), KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (utility model), SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) **Designated States** *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:

— *With international search report.*

— *Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SYSTEM AND METHOD FOR STORING, MANAGING, AND RETRIEVING HEALTHCARE INFORMATION ON A SMART CARD

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to a system and method for storing, managing, and retrieving healthcare information, more particularly, to a system and method for storing, managing, and retrieving healthcare information on a smart card.

2. Description of the Prior Art

When providing healthcare including routine health checks and various medical treatments, it is very important to know a patient's medical and health history, current drug regimen, and any current treatments. Patients frequently require a treatment by someone other than their primary care provider. Whether this treatment occurs in a hospital emergency room, a clinic across town, or in another state, access to a patient's medical and health information may not be readily available.

Some existing healthcare record systems use a patient ID card to locate patient's medical or health information stored in a care provider's own database. This type of ID card contains patient's general information, such as a patient's name, address, ID number, birthday, etc. The ID card does not contain any medical or health information. Also, such ID card is often proprietary, which is issued and used by the patient's primary care provider. Another care provider or paramedic/emergency team is not able to use the card to efficiently obtain the medical or health history of a patient.

In addition, this type of ID card may not be able to promptly record a current medical or health treatment provided by a healthcare provider other than a patient's primary care provider. Further, patients have to repeatedly register their general information every time they go to a different care provider. Furthermore, patients have to bring a different card every time when they go to see a different care provider.

There are many concerns related to using an ID card in a patient's healthcare record system. One main concern is patient's privacy if an ID card contains healthcare information. It is important to make sure that only certain authorized persons, such as a patient, a primary doctor, a pharmacist, a paramedic, etc., can access, update, or delete information in a patient's database. Also, it is important that the scope of authorization is defined such that only certain portions of a patient's database can be accessed, updated, or deleted by authorized persons. For

example, a patient may only be authorized to read certain test data file or lab result file, or update certain patient's general information, such as a current address, etc. A pharmacist may only be authorized to access a prescription file of the patient's database.

Another concern related to a patient's healthcare record system is how to efficiently manage and maintain patient's healthcare information. As mentioned above, healthcare providers have created their own databases to store patient healthcare information. These databases are generally designed for a particular care provider. As a result, these databases are often different and do not interface with each other. Thus, it is difficult to store, manage, or maintain a patient's specific healthcare record system in a ubiquitous manner. Care providers often do not have prompt access to a patient's vital medical or health information. Also, care providers are not able to promptly update a current healthcare treatment on a patient into the system. As a result, another care provider may not be able to access the most current healthcare information about this patient.

A further concern related to a patient's healthcare record system is the easy access issue. A patient often wants to access certain information, for example, the recent test report, etc. The existing systems do not provide such easy access. Thus, it is difficult for a patient or an authorized party to monitor a patient's health condition. On the other hand, there is a desire to have a fundamental paradigm shift in a healthcare record system from a care provider or institution owned patient's healthcare record system to a patient owned patient's healthcare record system.

Technology, such as the Internet, Smart Cards, etc., has availed itself to the healthcare industry and has become the driving force to revolutionize a patient's healthcare record system.

It is with respect to these and other considerations that the present invention has been made.

SUMMARY OF THE INVENTION

To overcome the limitations in the prior art described above, and to overcome other limitations that will become apparent upon reading and understanding the present specification, the present invention discloses a patient healthcare record system and method for storing, managing, and retrieving healthcare information on a smart card.

The present invention provides a method of storing, managing, and retrieving information in a record system via a smart card. In one embodiment, the method includes entering information at a first location, entering a smart card PIN at the first location, and issuing the smart card which stores at least a portion of the

information and the smart card PIN. The information and the smart card PIN are stored on a server of the record system. The smart card stores a flat file which is accessed via a database interface. The database interface converts the flat file stored on the smart card into a database file.

Still in one embodiment, the method further includes accessing the information at the first location by reading the smart card via a smart card reader at the first location. After an update at the first location, the method further includes storing a record of the update on the server, and storing at least a portion of the record of the update on the smart card.

Further in one embodiment, the method further includes accessing the information at a second location by reading the smart card via a smart card reader at the second location. After an update at the second location, the method further includes storing a record of the update on the server, and storing at least a portion of the record of the update on the smart card.

The present invention also provides a patient specific healthcare record system in an accessible, portable, and secure manner. In one embodiment, the system includes: a smart card having a processor, an operating system, and at least one file; a smart card reader operable to read/write the smart card; a computer coupled to the smart card reader, the computer having a processor, an operating system, a smart card application operable to convert the at least one file on the smart card to a smart card database file, and a system database file. The smart card database file is a subset of the system database file. The smart card database file may contain a security code to access the system database file.

Still in one embodiment, the computer includes a lost card database file that is a subset of the system database file and is a copy of the smart card database file.

In another embodiment of the present invention, a patient specific healthcare record system includes: a smart card having a processor, an operating system, and at least one file; a smart card reader operable to read/write the smart card; a client computer coupled to the smart card reader, the client computer having a processor, an operating system; a server computer coupled to the client computer, the server computer having a processor, an operating system, a smart card application operable to convert the at least one file on the smart card to a smart card database file, and a system database file. The smart card database file is a subset of the system database file and accessible via the client computer. The smart card database file may contain a security code to access the system database file.

Still in another embodiment, the server computer includes a lost card database file that is a subset of the system database file and is a copy of the smart

card database file. The client computer and the server computer are coupled in a network, such as a Local Area Network (LAN) or a Wide Area Network (WAN), etc.

In another embodiment of the present invention, a patient specific healthcare record system includes: a smart card having a processor, an operating system, and at least one file; a smart card reader operable to read/write the smart card; a web browser device coupled to the smart card reader, the web browser device having a processor and an operating system and being operable to browse the Internet; an Internet web portal/server coupled to the web browser device, the Internet web portal/server having a processor, an operating system, a system database file, and a smart card application operable to convert the at least one file on the smart card to a smart card database file. The smart card database file is a subset of the system database file and accessible via the web browser device. The smart card database file may contain a security code to access the system database file.

Still in another embodiment, the Internet web portal/server includes a lost card database file that is a subset of the system database file and is a copy of the subset of the system database file.

Further in another embodiment, the system further includes a second smart card having a processor, an operating system, and a key data file, the smart card application being operable to access a second subset of the system database file based on the key data file of the second smart card, the web browser device browsing the second subset of the system database file.

Yet in one embodiment of the present invention, the system further includes an Internet ancillary service web portal/server having a processor, an operating system, and a data file, the Internet ancillary service web portal/server being communicable with the Internet web portal/server, and the web browser device browsing the data file of the Internet ancillary service web portal/server.

Still in another embodiment, the data file stored on the smart card is a key data file. The patient's actual medical records are not stored on the smart card, but are stored in a database on a server. The key data file provides a key or security code to access the database on the server.

Accordingly, an authorized user having a smart card can access, update, and/or delete patient's healthcare records stored on the smart card. The authorized users can be the patient's primary care provider, paramedic, pharmacist, the patient's care provider other than the primary care provider, patient, smart card issuer, system administrator, etc. Such authorization can be implemented in one embodiment by granting access to such a user using another smart card and verifying a security code entered by the user. Once the system verifies the entered security

code by reading the user's smart card, the user can access an authorized portion of the smart card database file. If the authorized users are patients themselves, the authorization can be implemented in one embodiment by entering the patients' PINs, etc.

Therefore, the present invention provides ubiquitous access, at the point of care, to the patient's healthcare records stored on a smart card and/or the patient's healthcare records, if authorized, via a computer, a server computer in a network, or the Internet web portal/server on the Internet. Whenever or wherever a patient is given a treatment by a care provider, the care provider can promptly access and update the patient's healthcare records stored on his/her smart card and/or the patient's healthcare record, if authorized, stored on a computer, a LAN server, or the Internet web portal/server. The record of such treatment is appended to the previously recorded medical records such that another care provider or institution can later review the updated records in a subsequent treatment. Thus, the patient's healthcare records are generated and maintained from a patient's perspective rather than from a care provider or institution's perspective.

Also, the present invention provides other functionality on the smart card along with the patient specific healthcare record database. For example, a smart card may be used as a security key, or an electronic purse to allow quick and efficient medical payments (e.g. co-pay).

In addition, the present invention may provide a method of tracking specific population segments that are high risk, high usage, and high cost of a certain medical or health treatment. The population segments may be defined according to patient demographics and/or clinical histories. Examples of high-risk patients may include oncology, diabetes, asthma, or cardiology patients. Examples of high usage patients may include maternity patients during a pregnancy period. Examples of high cost patients may include a well child group, or children within the ages of 0-13 years.

Further, the present invention may provide a care provider a user-friendly interface on a patient's vital medical or health information, as opposed to a longitudinal list of medical records. Using this information, the care provider is capable of making an adequate assessment of the patient's medical condition. In one example, the database fields displayed at the user interface would not include the patient's complete healthcare records, but rather the vital medical information would be included therein. Most data entries in the database fields may be pre-defined and limited to specific categories.

These and various other advantages and features of novelty which characterize the invention are pointed out with particularity in the claims annexed

hereto and form a part hereof. However, for a better understanding of the invention, its advantages, and the objects obtained by its use, reference should be made to the drawings which form a further part hereof, and to accompanying descriptive matter, in which there are illustrated and described specific examples of an apparatus in accordance with the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

Referring now to the drawings in which like reference numbers represent corresponding parts throughout:

FIG. 1 is a block diagram showing one embodiment of a patient healthcare record system in accordance with the principles of the present invention.

FIG. 2 is a block diagram showing a second embodiment of a patient healthcare record system in accordance with the principles of the present invention.

FIG. 3 is a block diagram showing a third embodiment of a patient healthcare record system in accordance with the principles of the present invention.

FIG. 4 is a block diagram showing a fourth embodiment of a patient healthcare record system in accordance with the principles of the present invention.

FIG. 5 is a flow chart diagram showing a method of storing patient's information and issuing a new patient's smart card in accordance with the principles of the present invention.

FIG. 6 is a flow chart diagram showing a method of accessing and updating a return patient's smart card by a care provider in accordance with the principles of the present invention.

FIG. 7 is a flow chart diagram showing a method of accessing and updating a referral patient's smart card by a care provider in accordance with the principles of the present invention.

FIG. 8 is a flow chart diagram showing a method of accessing and updating a patient's smart card by an authorized paramedic/emergency team in accordance with the principles of the present invention.

FIG. 9 is a flow chart diagram showing a method of accessing and updating a patient's smart card by the patient in accordance with the principles of the present invention.

FIG. 10 is a flow chart diagram showing a method of accessing a lost card database and issuing a new smart card in accordance with the principles of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention relates to a patient specific healthcare system and method for storing, managing, and retrieving healthcare information on a smart card.

The present invention discloses a patient healthcare record system and method of storing, managing, and retrieving healthcare information on a smart card. The system allows healthcare providers to electronically capture, store and subsequently recall sufficient details concerning a patient's medical and health history to formulate a treatment plan. Rather than storing the healthcare information in a database accessible to a limited population, the system in accordance with the principles of the present invention provides the tools for storing and maintaining the information on a smart card. The smart card is generally controlled and carried by a patient. Given the disparate nature of healthcare delivery systems, the portability of information stored on the smart card can be used to improve the quality of care by making the healthcare information available at the point of care.

The system in accordance with the principles of the present invention is developed for different user classes, ranging from large hospitals or institutions that would tend to maintain their own patient information, to small clinics or individuals that would rely on other hospitals' or institutions' information.

In addition to storing, managing, and retrieving patient's healthcare information, smart cards also represent a suitable technology for storing digital certificates which, when used with biometrics identification, can be used to authenticate a cardholder's identity. Once identified, the cardholder can then be granted access to extended privileges, such as access to areas on the Internet web portal server not accessible to the general public information.

The system in accordance with the present invention may provide at least the following applications:

1) Smart card technology, in addition to storing, managing, and retrieving patients' healthcare information, for securing and limiting access by user classification to the patients' healthcare information.

2) Web-enabled applications allowing care providers to capture and quickly update patients' healthcare information without substantially altering their existing workflow.

3) Application extensions supporting at-risk patient populations including maternity, well child/immunization, geriatrics, diabetes, cardiology, oncology and asthma.

4) An enterprise-ready smart card issuance and tracking system including a lost card database or smart card life-cycle management.

5) An institutional smart card/patient tracking system (e.g. a local institutional database for tracking a patient healthcare record).

6) An Internet web portal server that extends the value of a smart card to a patient and a care provider by providing content that is tailored to the patient's specific healthcare background and interests.

7) Interfaces facilitating the exchange of patient information, including lab and radiology reports.

In the following description of the exemplary embodiment, reference is made to the accompanying drawings that form a part hereof, and in which is shown by way of illustration the specific embodiment in which the invention may be practiced. It is to be understood that other embodiments may be utilized as structural changes may be made without departing from the scope of the present invention.

In Figure 1, there is generally illustrated by reference numeral 20, one embodiment of a patient healthcare system in accordance with the principles of the present invention. The patient healthcare system 20 includes a smart card 22 having a CPU 24, an operating system (O/S) 26, and a plurality of flat files 28. The flat files 28 are one patient's healthcare records. The term, "flat files", is used to refer to files that are not associated with each other in a database structure. A smart card application, for example a smart card application using a database interface, such as an Object Linking and Embedding Database (OLE DB) 30 which is described later in detail, is used to link the flat files 28 such that a user is able to view the records in a database format. The smart card application 30 is stored and operated at a PC 32 shown in Figure 1, a server PC 34 shown in Figure 2, or an Internet web portal/server 36 shown in Figures 3 and 4.

In Figure 1, the system 20 also includes a smart card reader 38 operable to read/write the smart card 22. The smart card reader 38 provides smart card read/write capabilities and is known in the art to read and/or write the smart card 22. The PC 32 operates the smart card reader 38 so that the files 28 on the smart card 22 are loaded into the PC or vice versa. It is appreciated that the smart card reader 38 can be assembled as a part of the PC 32. For example, the smart card reader 38 can be implemented as an I/O device of the PC 32, such as a keyboard, PCMIC port, etc. The smart card reader 38 may also be implemented in a handheld CE type device.

The PC 32 includes a processor (not shown) which operates the smart card application 30. A patient healthcare database 40 and a lost card database 42 are stored in the PC 32. The patient healthcare database 40 is a patient healthcare database including all the patients registered in the system 20. A specific patient's

healthcare records are stored and updated in the patient healthcare database 40. The database generated from the flat files 28 on a specific patient's smart card 22 is a subset of the patient's healthcare records stored in the patient healthcare database 40.

The records on the smart card 22 are stored and updated by an authorized class of users, such as a patient, a care provider, or a smart card database administrator. For example, a patient may be authorized to update a certain fields of the database, such as the patient's current address, insurance information, emergency contact person, etc. A care provider may be authorized to update patient's healthcare records in a certain fields of the database once a new diagnosis or treatment is performed. A smart card database administrator may be authorized to validate a user's access to the files 28 on the smart card 22 and/or the database 40,42 on the PC 32, PC server 34, or web portal/server 36.

The records in the lost card database 42 are a copy of the records in the flat files 28 stored on the smart card 22. Thus, the lost card database 42 is also a subset of the patient's healthcare records stored in the patient healthcare database 40. The lost card database 42 is used in issuing a new smart card if the smart card 22 is lost. The most recent updated records in the lost card database 42 are stored on the new smart card. Preferably, only the smart card database administrator has the access to the lost card database. The smart card database administrator may update the system to validate the new smart card.

As shown in Figure 1, the lost card database 42 is a separate database from the patient healthcare database 40. It is appreciated that the lost card database 42 can be implemented as a part of the patient healthcare database 40 within the scope of the present invention.

In Figure 2, there is generally illustrated by reference numeral 44, a second embodiment of a patient healthcare system in accordance with the principles of the present invention. In Figure 2, same reference numerals are used for the corresponding parts of the system 20 in Figure 1 for the purpose of illustration. The patient healthcare system 44 includes a client PC 46 coupled to the smart card reader 38 and the server PC 34. The client PC 46 has a processor and an operating system (not shown). The server PC 34 has a processor and an operating system and is in a network communication with a plurality of client PCs 46. Each of the client PCs 46 has the capability of coupling to a smart card reader.

Also in Figure 2, the smart card application 30, the patient healthcare database 40, and the lost card database 42 are stored and operated on the server PC 34. Each of the client PCs 46 is capable of operating the smart card application 30, accessing the patient healthcare database 40, and the lost card database 42 on the server PC 34 so that the system 44 is ubiquous to each of the client PCs 46 in the

network. It is appreciated that the network can be a Local Area Network (LAN) or a Wide Area Network (WAN), etc., or a World Wide Web (WWW), etc. The WWW network is further explained as an example in Figures 3 and 4.

In Figure 3, there is generally illustrated by reference numeral 48, a third embodiment of a patient healthcare system in accordance with the principles of the present invention. In Figure 3, same reference numerals are used for the corresponding parts of the systems 20 and 44 in Figures 1 and 2 for the purpose of illustration. The patient healthcare system 48 includes a smart card 50 having the CPU 24, the operating system (O/S) 26, and a key data file 52. The key data file 52 may include an access code to allow a user to access a certain authorized portion of the patient healthcare database 40 or the lost card database 42. The key data file 52 is read by the smart card application 30 and is operable to retrieve the authorized portion of the patient healthcare database 40. The lost card database 42 includes a copy of the key data file 52 so that when a new smart card is issued to replace the lost smart card 50, the lost card database 42 is copied onto the new smart card. In an alternative embodiment, the key data file 52 may be maintained by a separate key management system. In this case, when a new smart card is issued, a copy of the key data file which is maintained by a separate key management system is stored on the new smart card.

In Figure 3, the system 48 also includes a web browser device 54, such as a PC or a handheld device, etc., having a processor and an operating system (not shown). The web browser device 54 is operable to browse the Internet and communicable with the Internet web portal/server 36. The web browser device 54 is coupled to the smart card reader 38 to read/write the smart card 50. The Internet web portal/server 36 can be implemented as a PC at an Internet service provider or a workstation, etc. The Internet web portal/server 36 has a processor and an operating system (not shown) and is in communication with a plurality of web browser devices 54 coupled to the Internet. The smart card application 30, the patient healthcare database 40, and the lost card database 42 are stored and operated on the Internet web portal/server 36. Each of the web browser devices 54 is capable of accessing the smart card application 30, accessing the patient healthcare database 40, and the lost card database 42 on the Internet web portal/server 36 so that the system 48 is ubiquous to each of the web browser devices 54.

Also in Figure 3, the Internet web portal/server 36 may be coupled to a plurality of Internet ancillary services 56 (only one is shown for illustration purposes). Each of the Internet ancillary services 56 is provided on an Internet web portal/server 58. The Internet ancillary services 56 may include a web site or chat room for advising treatments to a specific disease, diet programs, or exercise

programs. A user of the smart card 50 may access the contents of the Internet ancillary services 56 via the web browser device 54.

Further in Figure 3, an exemplary user profile of the system 48 is shown. One group of the users of the system 48 is patients 60 who hold the smart cards 50. Another group is patients' primary care providers 62 who provide primary medical/health care for the patients 60. An additional group can be clinic/general physicians 64 who are care providers other than the patients' primary care providers. Still another group can be pharmacists or other similar outpatient service providers 66 who supply patients' medications or other similar functions. Yet another group can be emergency teams/paramedics 68 who provide emergent, first response medical care for the patients. Further another group may be lost card administrators 70 who issue new smart cards to the patients who lost the smart cards. Still another group may be smart card issuers 72 who initially issue smart cards to the patients. It is appreciated that there may be other groups who are authorized to access the system 48 within the scope of the present invention. It is also appreciated that the above-mentioned groups can be integrated to perform multiple functions. For example, the smart card issuers 72 can be the same people as the lost card administrators 70 without departing from the principles of the present invention.

In using the system 48, the patient/smart cardholder 60 enters a security code, for example, a Personal Identification Number (PIN), a biometric identification, and/or a password, etc. Upon verification of the entered security code using the key data file 52, the patient/smart cardholder 60 is able to access an authorized portion or field of the patient healthcare records stored on the Internet web portal/server 36. The portion or field that a patient is authorized to access may be defined in a database which stores the access rules of various users. Database field definition technique is well known in the database art. Accordingly, a patient may be able to view certain information such as the lab test results, recent medical treatment, and ancillary services, etc. The patient may also be able to update the patient's general information as mentioned above.

If the user of the system is the primary care provider 62, the primary care provider 62 inserts the patient's smart card 50 and a primary care provider's own smart card 72 in the smart card reader 38. Upon verification of the entered security code using a key data file 74 of the primary care provider's smart card 72 and the key data file 52 of the patient's smart card 50, the primary care provider 62 is able to access an authorized portion or field of the patient healthcare records stored on the Internet web portal/server 36. The portion or field that a primary care provider is authorized to access may be defined in a database which stores the access rules of various users. The primary care provider 62 may be able to view patient's healthcare

records and update current treatments, conditions, and/or prescriptions, etc. Since the system 48 is ubiquous, the primary care provider is also able to view the past treatments, conditions, and/or prescriptions made by the clinic/general physicians 64 in a prompt manner.

Similarly, the clinic/general physician 64 may insert the patient's smart card 50 and the clinic/general physician's own smart card 76 in the smart card reader 38. Upon verification of the entered security code using a key data file 78 of the clinic/general physician's smart card 76 and the key data file 52 of the patient's smart card 50, the clinic/general physician's 64 is able to access an authorized portion or field of the patient healthcare records stored on the Internet web portal/server 36. The portion or field that the clinic/general physician is authorized to access may be defined in a database which stores the access rules of various users. The clinic/general physician 64 may be able to view patient's healthcare records and update current treatments, conditions, and/or prescriptions, etc. Since the system 48 is ubiquous, the clinic/general physician 64 is also able to view the past treatments, conditions, and/or prescriptions made by the primary care provider or the other clinic/general physicians 64 in a prompt manner.

If the user of the system 48 is the pharmacist/outpatient service 66, the pharmacist/outpatient service 66 inserts the patient's smart card 50 and the pharmacist/outpatient service's own smart card 80 in the smart card reader 38. Upon verification of the entered security code using a key data file 82 of the pharmacist/outpatient service's own smart card 80 and the key data file 52 of the patient's smart card 50, the pharmacist/outpatient service 66 is able to access an authorized portion or field of the patient healthcare records stored on the Internet web portal/server 36. The portion or field that the pharmacist/outpatient service 66 is authorized to access may be defined in a database which stores the access rules of various users. The pharmacist/outpatient service 66 may be able to view patient's prescription, insurance company, etc., and update the information of the prescribed medication. Since the system is ubiquous, the pharmacist/outpatient service 66 is able to view and update the above information in a prompt manner.

If the user of the system 48 is the paramedics/emergency team 68, the paramedics/emergency team 68 inserts the patient's smart card 50 and the paramedics/emergency team own smart card 84 in the smart card reader 38. Upon verification of the entered security code using a key data file 86 of the paramedics/emergency team own smart card 84 and the key data file 52 of the patient's smart card 50, the paramedics/emergency team 68 is able to access an authorized portion or field of the patient healthcare records stored on the Internet web portal/server 36. The portion or field that the paramedics/emergency team 68 is

authorized to access may be defined in a database which stores the access rules of various users. The paramedics/emergency team 68 may be able to view patient's prescription and recent medical treatment and condition records, etc., and update their treatments, observed conditions, etc. Since the system 48 is ubiquous, the paramedics/emergency team 68 is able to view and update the above information in a prompt manner.

If the user of the system 48 is the lost card administrator 70, the lost card administrator 70 inserts the lost card administrator own smart card 88 in the smart card reader 38. Upon verification of the entered security code using a key data file 90 of the lost card administrator own smart card 88, the lost card administrator 70 is able to access the lost card database 42 and an authorized portion or field of the patient healthcare records stored on the Internet web portal/server 36, for example, the portion or field that validates the new smart card. The portion or field that the lost card administrator 70 is authorized to access may be defined in a database which stores the access rules of various users.

If the user of the system 48 is the smart card initial issuer 72, the smart card initial issuer 72 inserts the smart card initial issuer's own smart card 92 in the smart card reader 38. Upon verification of the entered security code using a key data file 94 of the smart card initial issuer's own smart card 92, the smart card initial issuer 72 is able to enter patient's registration information into the patient's healthcare database 40, define which user is authorized to access/read/write which portions or fields of the patient's healthcare database 40, the key data file 52, and the lost card database 42, define which portions or fields of the key data file 52 should be stored on the smart card 50, the patient healthcare database 40, and the lost card database 42, store the information on the smart card 50, and validate the smart card 50, etc.

In Figure 4, there is generally illustrated by reference numeral 96, a fourth embodiment of a patient healthcare system in accordance with the principles of the present invention. The patient healthcare system 96 in Figure 4 is an alternative embodiment of the patient healthcare system 48 in Figure 3 where the patient's smart card 50 has the flat files 28 instead of the key data file 52 as shown in Figure 3. In Figure 4, same reference numerals are used for the corresponding parts of the systems 20, 44, and 48 in Figures 1-3 for the purpose of illustration. The patient healthcare system 96 includes a smart card 50 having the CPU 24, the operating system (O/S) 26, and flat files 28. The flat files 28 are operable with the smart card application 30 using a database interface, such as an Object Linking and Embedding Database (OLE DB). To a viewer, the flat files 28 are presented in a database format (referred to as a flat file database 28). The web browser device 54

browses the flat file database 28. The flat file database 28 may also include a field that authorizes the retrieval of a portion of the patient healthcare database 40.

The lost card database 42 stored on the Internet web portal/server 36 includes a copy of the flat file database 28 so that when a new smart card is issued to replace the lost smart card 50, the lost card database 42 belonged to the patient is copied onto the new smart card.

In Figure 4, the user profile of the system 96 is similar to that is shown in Figure 3. One group of the users of the system 96 is patients 60 who hold the smart cards 50. Another group is patients' primary care providers 62 who provide primary medical/health care for the patients 60. An additional group can be clinic/general physicians 64 who are care providers other than the patients' primary care providers. Still another group can be pharmacists or other similar outpatient service providers 66 who supply patients' medications or other similar functions. Yet another group can be emergency teams/paramedics 68 who provide emergent, first response medical care for the patients. Further another group may be lost card administrators 70 who issue new smart cards to the patients who lost the smart cards. Still another group may be smart card issuers 72 who initially issue smart cards to the patients. It is appreciated that there may be other groups who are authorized to access the system 96 within the scope of the present invention. It is also appreciated that the above groups can be integrated to perform multiple functions. For example, the smart card issuers 72 can be the same people as the lost card administrators 70 without departing from the principles of the present invention.

In using the system 96, the patient/smart cardholder 60 enters a security code, for example, a Personal Identification Number (PIN), a biometric identification, and/or a password, etc. Upon verification of the entered security code, the patient/smart cardholder 60 is able to access an authorized portion or field of the patient healthcare records stored on the Internet web portal/server 36. The portion or field that a patient is authorized to access may be defined in a database which stores the access rules of various users. A patient may be able to view certain information, for example, the lab test results, recent medical treatment, and/or ancillary services 56, etc. The patient may also be able to update the patient's general information, for example, the current address, etc. The flat file database 28 is then updated. Once the discrepancy among the flat file database 28, the subset of the patient healthcare database 40, and/or the lost card database 42 is detected, the patient healthcare database 40 and/or the lost card database 42 are updated automatically. Alternatively, a warning or notice may be presented to the user on the web browser device 54 to ask the user whether an update should be made in the patient healthcare database 40 immediately. The user enters yes or no. If the entry

is yes, the update is made immediately, and the lost card database 42 is automatically updated immediately. If the entry is no, the update is put on hold until next time the smart card 50 is used. It is appreciated that the synchronization between the flat file database 28 stored on the smart card 50 and the patient healthcare database 40 stored on the Internet web portal/server 36 can be implemented in a variety of ways within the scope of the present invention.

If the user of the system 96 is the primary care provider 62, the primary care provider 62 inserts the patient's smart card 50 and a primary care provider's own smart card 72 in the smart card reader 38. Upon verification of the entered security code using a key data file 74 of the primary care provider's smart card 72 and the flat file database 28 of the patient's smart card 50, the primary care provider 62 is able to access an authorized portion or field of the flat file database 28 and an authorized portion or field of the patient healthcare records stored on the Internet web portal/server 36. The portion or field that a primary care provider is authorized to access may be defined in a database which stores the access rules of various users. The primary care provider 62 may be able to view patient's healthcare records and update current treatments, conditions, and/or prescriptions, etc. Since the system 96 is ubiquous, the primary care provider 62 is also able to view the past treatments, conditions, and/or prescriptions made by the clinic/general physician 64 in a prompt manner.

Similarly, the clinic/general physician 64 may insert the patient's smart card 50 and the clinic/general physician's own smart card 76 in the smart card reader 38. Upon verification of the entered security code using a key data file 78 of the clinic/general physician's smart card 76 and the flat file database 28 of the patient's smart card 50, the clinic/general physician's 64 is able to access an authorized portion or field of the flat file database 28 and an authorized portion or field of the patient healthcare records stored on the Internet web portal/server 36. The portion or field that the clinic/general physician is authorized to access may be defined in a database which stores the access rules of various users. The clinic/general physician 64 may be able to view patient's healthcare records and update current treatments, conditions, and/or prescriptions, etc. Since the system 96 is ubiquous, the clinic/general physician 64 is also able to view the past treatments, conditions, and/or prescriptions made by the primary care provider 62 or the other clinic/general physician in a prompt manner.

If the user of the system 96 is the pharmacist/outpatient service 66, the pharmacist/outpatient service 66 inserts the patient's smart card 50 and the pharmacist/outpatient service's own smart card 80 in the smart card reader 38. Upon verification of the entered security code using a key data file 82 of the

pharmacist/outpatient service's own smart card 80 and the flat file database 28 of the patient's smart card 50, the pharmacist/outpatient service 66 is able to access an authorized portion or field of the flat file database 28 and an authorized portion or field of the patient healthcare records stored on the Internet web portal/server 36. The portion or field that the pharmacist/outpatient service 66 is authorized to access may be defined in a database which stores the access rules of various users. The pharmacist/outpatient service 66 may be able to view patient's prescription, insurance company, etc., and update the information of the prescribed medication. Since the system 96 is ubiquous, the pharmacist/outpatient service 66 is able to view and update the above information in a prompt manner.

If the user of the system 96 is the paramedics/emergency team 68, the paramedics/emergency team 68 inserts the patient's smart card 50 and the paramedics/emergency team own smart card 84 in the smart card reader 38. Upon verification of the entered security code using a key data file 86 of the paramedics/emergency team own smart card 84 and the flat file database 28 of the patient's smart card 50, the paramedics/emergency team 68 is able to access an authorized portion or field of the flat file database 28 and an authorized portion or field of the patient healthcare records stored on the Internet web portal/server 36. The portion or field that the paramedics/emergency team 68 is authorized to access may be defined in a database which stores the access rules of various users. The paramedics/emergency team 68 may be able to view patient's prescription and recent medical treatment and condition records, etc., and update their treatments, observed conditions, etc. Since the system 96 is ubiquous, the paramedics/emergency team 68 is able to view and update the above information in a prompt manner.

If the user of the system 96 is the lost card administrator 70, the lost card administrator 70 inserts the lost card administrator own smart card 88 in the smart card reader 38. Upon verification of the entered security code using a key data file 90 of the lost card administrator own smart card 88, the lost card administrator 70 is able to access the lost card database 42, an authorized portion or field of the flat file database 28, and an authorized portion or field of the patient healthcare records stored on the Internet web portal/server 36, for example, the portion or field that validates the new smart card. The portion or field that the lost card administrator 70 is authorized to access may be defined in a database which stores the access rules of various users.

If the user of the system 96 is the smart card initial issuer 72, the smart card initial issuer 72 inserts the smart card initial issuer's own smart card 92 in the smart card reader 38. Upon verification of the entered security code using a key data file 94 of the smart card initial issuer's own smart card 92, the smart card initial

issuer 72 is able to enter patient's registration information into the patient's healthcare database 40, define which user is authorized to access/read/write which portions or fields of the patient's healthcare database 40, flat file database 28, and the lost card database 42, define which portions or fields should be stored on the flat file database 28, the patient healthcare database 40, and/or the lost card database 42, store the information on the smart card, and validate the smart card, etc.

In the above and below examples, a care provider or smart card administrator uses his/her own smart card to gain access to the system and/or databases. It is appreciated that in alternative embodiments, instead of using his/her own smart card, a care provider or smart card administrator may access the system and/or databases via a variety of other methods, such as entering an authorized key code, or biometric identification, etc.

As an example, FIG. 5 shows a flow operation 98 of storing patient's information and issuing a new patient's smart card in accordance with the principles of the present invention. The operation 98 starts with an operation 100 of entering patient's general information in a new smart card data file. The entry can be done by a patient filling general information in a kiosk or a pre-printed paper form, and then by a care provider electronically scanning the general information into the new smart card data file or manually entering the general information into the new smart card data file. A patient selects a smart card PIN in an operation 102. Next, the patient authorizes emergency or first response access in the new smart card data file in an operation 104. After a medical examination, patient's medical information is then entered in the new smart card data file in an operation 106. Next, the new smart card data file is sent to a new smart card issuer in an operation 108. The new smart card issuer then issues a new smart card with a flat file database stored on the smart card in an operation 110. The flat file database on the smart card contains at least a portion of patient's new smart card data file, and the new smart card data file is stored on a PC, a PC server, or an Internet web portal/server. It is appreciated that the sequence of the flow operation 98 does not need to be in an order shown in FIG. 5. For example, the operation 102 of selecting a smart card PIN can be performed after the operation 104 of authorizing emergency, first response access. It is also appreciated that the operation 106 may be omitted if no treatment is performed.

As an example, FIG. 6 shows a flow operation 112 of accessing and updating a return patient's smart card by a care provider in accordance with the principles of the present invention. The operation 112 starts with an operation 114 of inserting a patient's smart card in a smart card reader at a care provider. Then, the flat file database stored on the patient's smart card is accessed in an operation 116. In another embodiment, the care provider may not be able to access the flat file

database on the smart card unless authorized. Next, the smart card reader reads a care provider's smart card to obtain authorization to access the patient's database stored on the server in an operation 118. Once authorized in the operation 118, the patient's medical information stored on the server is accessed in an operation 120. After the care provider provides a new treatment, the database stored on the server is updated in an operation 122, and the database stored on patient's smart card is updated in an operation 124. It is appreciated that the sequence of the flow operation 112 does not need to be in an order shown in FIG. 6. For example, the operation 124 of updating the database stored on patient's smart card can be performed before the operation 122 of updating the database stored on the server.

As an example, FIG. 7 illustrates a flow operation 126 of accessing and updating a referral patient's smart card by a care provider in accordance with the principles of the present invention. The operation 126 starts with an operation 128 of inserting a patient's smart card in a smart card reader at a care provider. Then, the patient's database stored on the smart card is accessed in an operation 130. In another embodiment, the care provider may not be able to access the flat file database store on the smart card unless authorized. Next, the smart card reader reads a care provider's smart card to obtain authorization to access the patient's database stored on the server in an operation 132. Once authorized in the operation 132, the patient's medical information stored on the server, for example, the medical information entered previously by another care provider, is accessed in an operation 134. After the care provider provides a new treatment, the database stored on the server is updated in an operation 136, and the database stored on patient's smart card is updated in an operation 138. It is appreciated that the sequence of the flow operation 126 does not need to be in an order shown in FIG. 7. For example, the operation 138 of updating the database stored on patient's smart card can be performed before the operation 136 of updating the database stored on the server.

As an example, FIG. 8 shows a flow operation 140 of accessing and updating a patient's smart card by an authorized paramedic/emergency team in accordance with the principles of the present invention. The operation 140 starts with an operation 142 of inserting emergency provider's smart card and patient's smart card to obtain authorization to access the patient's database stored on the smart card. If authorized, the patient's database stored on the smart card is accessed in an operation 144, and the patient's database stored on the server is accessed in an operation 146. After the emergency provider provides a new treatment, the database stored on the server is updated in an operation 148, and the database stored on patient's smart card is updated in an operation 150. It is appreciated that the sequence of the flow operation 140 does not need to be in an order shown in FIG. 8.

For example, the operation 150 of updating the database stored on patient's smart card can be performed before the operation 148 of updating the database stored on the server.

As an example, FIG. 9 illustrates a flow operation 152 of accessing and updating a patient's smart card by the patient in accordance with the principles of the present invention. The operation 152 starts with an operation 154 of inserting a patient's smart card to obtain authorization to access the database stored on the smart card. Then, the patient accesses the authorized portion of the database stored on the smart card in an operation 156. Next, the patient updates the flat file database in the authorized portion of the database stored on the smart card in an operation 158. Then, the database stored on the server is updated by the smart card application stored on the server in an operation 160. It is appreciated that the sequence of the flow operation 152 does not need to be in an order shown in FIG. 9.

As an example, FIG. 10 shows a flow operation 162 of accessing a lost card database and issuing a new smart card in accordance with the principles of the present invention. The operation 162 starts with an operation 164 of entering an administrator's identification to obtain authorization to a lost card database stored on a server. The administrator may enter a security code or insert an administrator smart card to obtain authorization. If authorized, the administrator enters patient's general information to search lost card database information of the patient stored on the server in an operation 166. Next, the administrator accesses the patient's lost card database stored on the server in an operation 168. Then, the administrator issues a new smart card with a flat file database stored on the smart card being the same as the lost card database in an operation 170. It is appreciated that the sequence of the flow operation 162 does not need to be in an order shown in FIG. 10.

The following description provides the implementation of one embodiment of: (I) a smart card of the patient's healthcare system; and (II) a smart card application using a database interface, such as an Object Linking and Embedding Database (OLE DB), of the patient's healthcare system in accordance with the principles of the present invention. It is noted that this and other implementations of the above-described system will be appreciated by a person skilled in the smart card art and the database art upon understanding of the present invention described above.

I. A smart card of the patient's healthcare system.

The patient's healthcare system is a combination of physical components, such as a smart card and a smart card software application. The physical components may also include a PC-based workstation and the associated

smart card reader. The smart card application may include a complete turnkey user interface package that provides the user all of the functionality required to capture data and store the data to both a database and a smart card. The following references are related to smart cards and are incorporated herein by reference:

- *ISO/IEC 7816-1: 1987, Identification cards - Integrated circuit(s) cards with contacts - Part 1: Physical characteristics*
- *ISO/IEC 7816-2: 1988, Identification cards - Integrated circuit(s) cards with contacts - Part 2: Dimensions and location of contacts*
- *ISO/IEC 7816-3: 1989, Identification cards - Integrated circuit(s) cards with contacts - Part 3: Electronic signals and transmission protocols*
- *ISO/IEC 7816-4: 1995, Identification cards - Integrated circuit(s) cards with contacts - Part 4: Inter-industry commands*
- *ISO/IEC 7816-5: 1994, Identification cards - Integrated circuit(s) cards with contacts - Part 5: Numbering system and registration procedure for application identifiers*
- *ISO/IEC 7816-6: 1994, Identification cards - Integrated circuit(s) cards with contacts - Part 6: Inter-industry data elements*
- *Interoperability Specification for ICCs and Personal Computer Systems - Part 1. Introduction and Architecture Overview*
- *Interoperability Specification for ICCs and Personal Computer Systems - Part 7. Application Domain and Developer Design Considerations*
- *ANSI NCITS.284-1997 Identification Cards - Health Care Identification Cards*
- *Interoperability Specification for ICCs and Personal Computer Systems*
- *Diving into the Requirements for the Windows 95 Logo white paper*

It is appreciated that other types of user identification devices or methods may be used within the scope of the present invention. For example, the system may include a biometrics capture device, such as an eye scan or a finger print identification device.

A flat file database is stored on the smart card. The flat file database may include a plurality of database fields. As an example, the database fields may include the following pre-defined properties:

1. Name: with a name including 1-32 alphanumeric and underscore characters.
2. Data type: text, numeric and/or date fields.
3. Length: maximum of 1-128 for text fields and decimal precision of 1-8 for numeric fields.
4. Index Field: off for all fields but those contained in the identification frame. Each table includes at least one index field.

An index is a specially defined database field by which the database stores records. Because databases store their records according to the indexed field's value, searching on indexed fields is much faster than on non-indexed fields.

5. Unique: off for all fields but the unique identifier. At least one index field is set to contain a unique value for each record.

The flat file database may also include a security code field. As an example, the security code field may be selected from the following sections:

1. Patient's ID number: 1-16 alphanumeric string. This is a unique identifier for each patient in the database.
2. Patient's social security number: zero length or 9-digit string with an input mask.
3. Last name: 1-20 character text string. This is a patient's last name.
4. First name: 1-20 character text string. This is a patient's first name.
5. Middle name: 0-20 character text string. This is a patient's middle initial or name.
6. Title: 0-16 character text string. This is a patient's pre-title (e.g. Mr., Mrs., Ms., Dr., Sir).
7. Suffix: 0-16 character text string. This is a patient's post-title (e.g. Jr., Sr., II, III, IV, PhD, DDS).
8. Birth date: stored in a yyyy/mm/dd format. This is a patient's birth date.
9. VIP type: one character value (B, D, P, E, C) to be displayed as one of the following, respectively: board member, donor level, planned donor (upon self or spouse's death), employee, chaplain.
10. VIP notification desired: yes/no toggle. This indicates whether or not the VIP patient would like healthcare administrators notified.

The flat file database may also include a personal contact field, an employment information field, an emergency contact field, an insurance information field, a guarantor information field, a patient's preference field (e.g. a preferred primary care physician information, a preferred hospital, a preferred pharmacy, living will information, organ donor information, or other demographic information), and a medical history field (such as allergies information, diabetes information, e.g. date of diagnosis, etc., past surgery information, e.g. the surgeon's name, etc., medication information, e.g. the refill frequency, etc., radiology and lab

test information, child and/or adult immunization information, maternity information if applicable, pregnancy information if applicable, past medical problems, e.g. seizure, etc.), etc.

A system administrator or database administrator may specify directories and sub-directories into which various data files and defaults can be stored and defined. The data files may include a user path name, an audit log path name, and a database path name.

II. A smart card application using a database interface, such as an Object Linking and Embedding Database (OLE DB), of the patient's healthcare system.

The patient healthcare system may be distributed with three DLLs (Dynamic Link Library): DSCOleDB.DLL, SCDBLib.DLL, and CommonDLL.DLL, that provide an OLE DB interface to a smart card to allow the system to use a smart card in the same way that it would use another database to store information. The following description is a description of these DLLs and how they relate to each other.

The smart card application is used for communication with a smart card. The smart card application may use a database interface, such as an Object Linking and Embedding Database (OLE DB), and is designed to allow database operations to be performed on a variety of data sources or flat files even if these data sources or flat files are not actually a database in a traditional sense. For instance, an application may communicate with a spreadsheet through the OLE DB provided that a spreadsheet vendor supplies a proper interface layer. Because the OLE DB architecture provides this type of flexibility, the OLE DB is used to store data on a smart card. With this design, the system is able to use a smart card for data storage in much the same way that it uses an Access database. All of the basic database operations, such as update and insert operations, are supported through a command interface. For example, the smart card OLE DB will return rowsets that can then be displayed and modified. Since the smart card application using an OLE DB is independent of the system core design, changes to the smart card application using an OLE DB do not require the system core design to be changed. For example, changing the type of smart card reader used and/or changing the type of smart cards used do not require changes in the source code of the smart card application using an OLE DB.

Secondly, the smart card application using an OLE DB provides more independence to the system. Also, the smart card application

using an OLE DB provides greater flexibility so as to minimize code changes in the smart card application.

As an example, the smart card application using an OLE DB includes several layers that perform different functions. The system can communicate with a top layer using, for example, Microsoft's OLE DB COM interfaces. In general, no layer beneath this one is accessed directly by other applications, and each layer only interacts with the layers above and below. One exception to this is the CommonDLL. The CommonDLL includes some functionality that is used by all of the other layers or components. Although these layers are largely independent of each other in terms of the functionality that they provide, there are some notable parallels between the different layers. For example, the interface that the OLE DB uses to communicate with a DSM (Data Store Manager) layer is similar to a layer that the DSM uses to communicate with an IOS (Input/Output Security) layer. In addition, a Standard Template Library (STL) is used throughout the layers and components.

The DSCOleDB of the OLE DB is to implement a set of OLE DB interfaces to allow database operations to be performed by an application. This may be the only layer that is generally accessible to an outside application. The application using an OLE DB performs several functions. Primarily, it is responsible for receiving and parsing commands. The commands include a small number of simple, proprietary or customized commands that perform database operations. For example, the five basic commands in a database, i.e., "select," "update," "insert," "delete" and "flush," are supported. Each of these commands, with the exception of the flush command, may be performed on a single table.

When these commands are received and parsed, appropriate DSM (Data Store Manager) objects are stored in memory, and the requested operations are performed on these objects. These objects represent data stores and tables on the smart card and are stored in memory until a "flush" operation is performed. Thus, for example, an "update" operation followed by a "flush" operation will change the appropriate information in the tables on the smart card.

The SCDBLib of the OLE DB includes the functionality and classes that are used by the OLE DB. The interface to the SCDBLib is not a COM interface. Instead, the classes and functions that are used by the OLE DB are exported from the DLL. Three distinct layers may exist within the

SCDBLib, each of which provides a different type of functionality. These layers are described below:

1. Data Store Manager (DSM) Layer

The DSM layer has three main purposes. First, this layer provides the decision-making logic that is used to determine what should and should not be stored on a smart card, as well as the format for the information that is stored on the smart card. For example, some fields provide information that is useful, but not critical. Since the amount of space available on the smart card is quite small compared to the amount of space that is available in the database, some fields that are stored in the database may not be stored on the smart card. In these cases, the DSM layer will not store the information on the card. In other cases, a field may be stored in the database in a manner that is straightforward, but inefficient. In such cases, the DSM layer may store the information in a format that is less straightforward, but takes up less room on the smart card. To the layers above the DSM layer, these format translations are transparent.

The second purpose of the DSM layer is to translate table names as they are requested by the application into table numbers that are used by the IOS layer below it, as well as dividing fields of tables into records. Since the IOS layer handles tables as raw sequences of data while the application handles data according to table names and field names, the DSM layer provides a bridge between these two different ways of representing the data.

The third purpose of the DSM layer is to provide versioning support. Since a single smart card can be carried between different medical facilities that may have different versions of the system, the DSM layer is able to translate between older and newer versions of the system. In other words, the DSM layer should be able to recognize information on the smart card that has been stored by an older version of the application and to return that information to the application in the format that the application expects. This should again be transparent to the layers above the DSM.

In order to perform these purposes in a way that is easily extensible, the data files or flat files and the relationships between items in the data files or flat files may not be coded into the software itself, but are kept in a separate ACCESS database, e.g. SCDBLbDM.mdb. Thus, when new components are added or fields are modified, the actual source code can remain unchanged.

The DSM layer includes the classes that are exported from the DLL to be used by the OLE DB. The three primary exported classes are the ReaderConnection class, the DataStoreConnection class, and the TableConnection class. These three classes provide an abstraction of the database operations that are performed by the application.

2. Input/Output/Security (IOS) Layer

The primary purpose of the IOS layer is to manage the directories that are stored on a smart card. The DSM layer requests information using the database abstractions data stores and tables. Since the card itself uses file system abstractions instead of database abstractions, this layer is responsible for bridging those two abstractions.

The IOS layer accepts table data in the form of tables composed of uniform-sized records. Each record may include a sequence of raw bytes and the IOS layer does not interpret this data in any way. Each record may be indexed by an unsigned integer. The directory and file abstractions allow for different smart cards to be used transparently with minimal changes to existing code.

3. PC/SC Layer

As an example, the Windows™ implementation of PC/SC uses a C-style API (Application Programming Interface) that provides support for the functionality described in a PC/SC standard. In order to make this interface easier to use within a C++ application, several C++ wrapper classes were written. The organization of these classes and their relationship to each other is based upon the PC/SC standard. The classes will translate error values that are returned by the API into exceptions.

Since the classes may be used in contexts other than that of the OLE DB, the PC/SC layer is largely independent of the layers above it.

It is appreciated that other layers may be used within the scope of the present invention. It is also appreciated the terminology, such as data tables, components, objects, etc., used in the above description for the smart card database interface is well known in the software art and can be found in reference books, such as the one entitled "Understanding ActiveX and OLE", by David Chappel, Microsoft Press, 1996.

The foregoing description of the exemplary embodiment of the invention has been presented for the purposes of illustration and description. It is not intended to be exhaustive or to limit the invention to the precise form disclosed. Many modifications and variations are possible in light of the above teaching. It is

intended that the scope of the invention be limited not with this detailed description, but rather by the claims appended hereto.

CLAIMS

What is claimed is:

1. A method of storing, managing, and retrieving healthcare information in a record system via a smart card, comprising:

entering healthcare information at a first location;

entering a smart card PIN at the first location; and

issuing the smart card which stores at least a portion of the healthcare information and the smart card PIN, and the healthcare information and the smart card PIN being stored on a server of the record system.

2. The method of claim 1, further comprising: accessing the healthcare information at the first location by reading the smart card via a smart card reader at the first location.

3. The method of claim 2, further comprising: after an update of the healthcare information at the first location, storing a record of the update on the server, and storing at least a portion of the record of the update on the smart card.

4. The method of claim 1, further comprising: accessing the healthcare information at a second location by reading the smart card via a smart card reader at the second location.

5. The method of claim 4, further comprising: after an update of the healthcare information at the second location, storing a record of the update on the server, and storing at least a portion of the record of the update on the smart card.

6. The method of claim 1, wherein the smart card stores a flat file which is accessed via a database interface, the database interface converts the flat file stored on the smart card into a database file.

7. A system for storing, managing, and retrieving a patient's healthcare record, comprising:

a smart card having a processor, an operating system, and at least one file;

a smart card reader operable to read/write the smart card; and

a computer coupled to the smart card reader, the computer having a processor, an operating system, a smart card application operable to convert the at least one file on the smart card to a smart card database file, and a system database file, the smart card database file being a subset of the system database file.

8. The system of claim 7, wherein the smart card database file contains a security code to access the system database file.

9. The system of claim 7, wherein the computer includes a lost card database file that is a subset of the system database file and is a copy of the smart card database file.

10. The system of claim 7, wherein the smart card application includes a database interface which converts the at least one file on the smart card to the smart card database file.

11. A system for storing, managing, and retrieving a patient's healthcare record, comprising:

a smart card having a processor, an operating system, and at least one file;

a smart card reader operable to read/write the smart card;

a client computer coupled to the smart card reader, the client computer having a processor, an operating system; and

a server computer coupled to the client computer, the server computer having a processor, an operating system, a smart card application operable to convert the at least one file on the smart card to a smart card database file, and a system database file, the smart card database file being a subset of the system database file and accessible via the client computer.

12. The system of claim 11, wherein the smart card database file contains a security code to access the system database file.

13. The system of claim 11, wherein the server computer includes a lost card database file that is a subset of the system database file and is a copy of the smart card database file.

14. The system of claim 11, wherein the client computer and the server computer are coupled in a Local Area Network (LAN).

15. The system of claim 11, wherein the smart card application includes a database interface which converts the at least one file on the smart card to the smart card database file.

16. A system for storing, managing, and retrieving a patient's healthcare record, comprising:

a smart card having a processor, an operating system, and at least one file;

a smart card reader operable to read/write the smart card;

a web browser device coupled to the smart card reader, the web browser device having a processor and an operating system and being operable to browse the Internet; and

an Internet web portal/server coupled to the web browser device, the Internet web portal/server having a processor, an operating system, a system database file, and a smart card application operable to convert the at least one file on the smart card to a smart card database file, the smart card database file being a subset of the system database file and accessible via the web browser device.

17. The system of claim 16, wherein the smart card database file contains a security code to access the system database file.

18. The system of claim 16, wherein the internet web portal/server includes a lost card database file that is a subset of the system database file and is a copy of the subset of the system database file.

19. The system of claim 16, further comprising a second smart card having a processor, an operating system, and a key data file, the smart card application being operable to access a second subset of the system database file based on the key data file of the second smart card, the web browser device browsing the second subset of the system database file.

20. The system of claim 19, wherein the smart card application includes a database interface which converts the at least one file on the smart card to the smart card database file.

21. The system of claim 16, further comprising: an Internet ancillary service web portal/server having a processor, an operating system, and a data file, the Internet ancillary service web portal/server being communicable with the Internet web portal/server, and the web browser device browsing the data file of the Internet ancillary service web portal/server.

22. A system for storing, managing, and retrieving a patient's healthcare record, comprising:

a smart card having a processor, an operating system, and a key data file;

a smart card reader operable to read/write the smart card; and

a computer coupled to the smart card reader, the computer having a processor, an operating system, a smart card application operable to access a subset of the system database file based on the key data file, and a system database file, the computer browsing the subset of the system database file based on the key data file.

23. The system of claim 22, wherein the key data file contains a security code to access the system database file.

24. The system of claim 22, wherein the computer includes a lost card database file that is a subset of the system database file and a copy of the subset of the system database file based on the key data file.

25. A system for storing, managing, and retrieving a patient's healthcare record, comprising:

a smart card having a processor, an operating system, and a key data file;

a smart card reader operable to read/write the smart card;

a client computer coupled to the smart card reader, the client computer having a processor, an operating system; and

a server computer coupled to the client computer, the server computer having a processor, an operating system, a smart card application operable to access a subset of the system database file based on the key data file, and a system database file, the client computer browsing the subset of the system database file based on the key data file.

26. The system of claim 25, wherein the key data file contains a security code to access the system database file.

27. The system of claim 25, wherein the server computer includes a lost card database file that is a subset of the system database file and is a copy of the subset of the system database file based on the key data file.

28. The system of claim 25, wherein the client computer and the server computer are coupled in a Local Area Network (LAN).

29. A system for storing, managing, and retrieving a patient's healthcare record, comprising:

a smart card having a processor, an operating system, and a key data file;

a smart card reader operable to read/write the smart card;

a web browser device coupled to the smart card reader, the web browser device having a processor and an operating system and being operable to browse the Internet;

an Internet web portal/server coupled to the web browser device, the Internet web portal/server having a processor, an operating system, a system database file, and a smart card application operable to access a subset of the system database file based on the key data file, the web browser device browsing the subset of the system database file based on the key data file.

30. The system of claim 29, wherein the internet web portal/server includes a lost card database file that is a subset of the system database file and is a copy of the subset of the system database file based on the key data file.

31. The system of claim 29, further comprising a second smart card having a processor, an operating system, and a key data file, the smart card application being operable to access a second subset of the system database file based on the key data files of the smart cards, the web browser device browsing the second subset of the system database file.

32. The system of claim 29, further comprising: an Internet ancillary service web portal/server having a processor, an operating system, and a data file, the Internet ancillary service web portal/server being communicable with the Internet web portal/server, and the web browser device browsing the data file of the Internet ancillary service web portal/server.

33. A method of storing patient's information and issuing a new patient smart card, comprising:

entering patient's general information in a new smart card data file;

selecting a smart card PIN;

authorizing emergency response access in the new smart card data file;

updating the patient's medical information after a medical treatment in the new smart card data file;

sending the new smart card data file to a new smart card issuer; and

issuing the new smart card with at least one data file stored on the smart card by the new smart card issuer, the at least one data file stored on the smart card

containing at least a portion of the new smart card data file, and the new smart card data file being stored on a server.

34. The method of claim 33, wherein entering of the patient's general information in the new smart card data file is accomplished by a patient providing the general information in a kiosk.

35. The method of claim 33, wherein entering of the patient's general information in the new smart card data file is accomplished by a patient providing the patient's general information in a pre-printed form, and by a care provider electronically scanning the patient's general information into the new smart card data file.

36. The method of claim 33, wherein entering of the patient's general information in the new smart card data file is accomplished by a patient providing the general information in a pre-printed form, and by a care provider manually entering the general information into the new smart card data file.

37. A method of accessing and updating a return patient's smart card by a care provider, comprising:

inserting a patient's smart card in a smart card reader at a care provider;

accessing at least one data file stored on the patient's smart card;

reading a care provider's smart card to obtain authorization to access a patient's database stored on a server;

accessing patient's medical information in the patient's database stored on the server, upon authorization; and

updating the patient's medical information after a medical treatment in the at least one data file stored on the patient's smart card.

38. The method of claim 37, further comprising updating the patient's medical information after the medical treatment in the patient's database stored on the server.

39. The method of claim 37, wherein accessing of the at least one data file stored on the patient's smart card is accessed upon authorization.

40. A method of accessing and updating a referral patient's smart card by a care provider, comprising:

inserting a patient's smart card in a smart card reader at a care provider;

accessing at least one data file stored on the patient's smart card;

reading a care provider's smart card to obtain authorization to access a patient's database stored on a server;

accessing patient's medical information stored on the server entered previously by another care provider, upon authorization; and

updating the patient's medical information after a medical treatment in the at least one data file stored on the patient's smart card.

41. The method of claim 40, further comprising updating the patient's medical information after the medical treatment in the patient's database stored on the server.

42. The method of claim 40, wherein accessing of the at least one data file stored on the patient's smart card is accessed upon authorization.

43. A method of accessing and updating a patient's smart card by an authorized paramedic/emergency team, comprising:

inserting an emergency provider's smart card and a patient's smart card to obtain authorization to access a patient's database stored on the patient's smart card;

accessing at least one data file stored on the patient's smart card, upon authorization;

accessing the patient's database stored on the server, upon authorization; and

updating patient's medical information, after the authorized paramedic/emergency team provides a medical treatment, in the at least one data file stored on the patient's smart card.

44. The method of claim 43, further comprising updating the patient's medical information after the medical treatment in the patient's database stored on the server.

45. The method of claim 43, wherein accessing of the at least one data file stored on the patient's smart card is accessed upon authorization.

46. A method of accessing and updating a patient's smart card by a patient, comprising:

inserting the patient's smart card to obtain authorization to access at least one data file stored on the patient's smart card;

accessing an authorized portion of the at least one data file stored on the smart card; and

updating an authorized portion of the at least one data file stored on the smart card.

47. The method of claim 46, further comprising updating an authorized portion of a patient's database stored on a server.

48. The method of claim 46, wherein accessing of the at least one data file stored on the smart card is accessed upon authorization.

49. The method of claim 47, wherein the patient's database stored on the server is updated by a smart card application stored on the server.

50. A method of accessing a lost card database and issuing a new smart card, comprising:

entering an administrator's identification to obtain authorization to access a lost card database stored on a server;

entering patient's general information, upon authorized, to search the lost card database stored on the server;

accessing patient's medical information in the lost card database stored on the server; and

issuing the new smart card containing at least one data file being the same as the lost card database.

Fig. 1

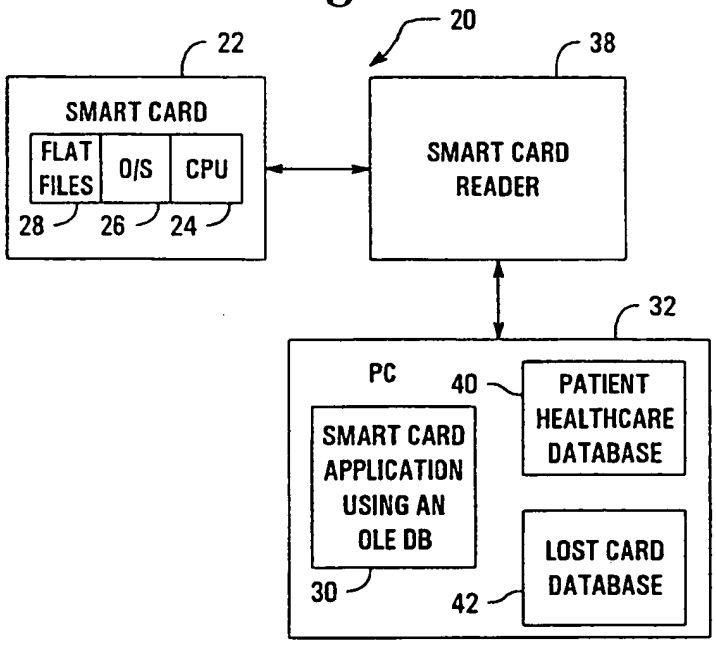
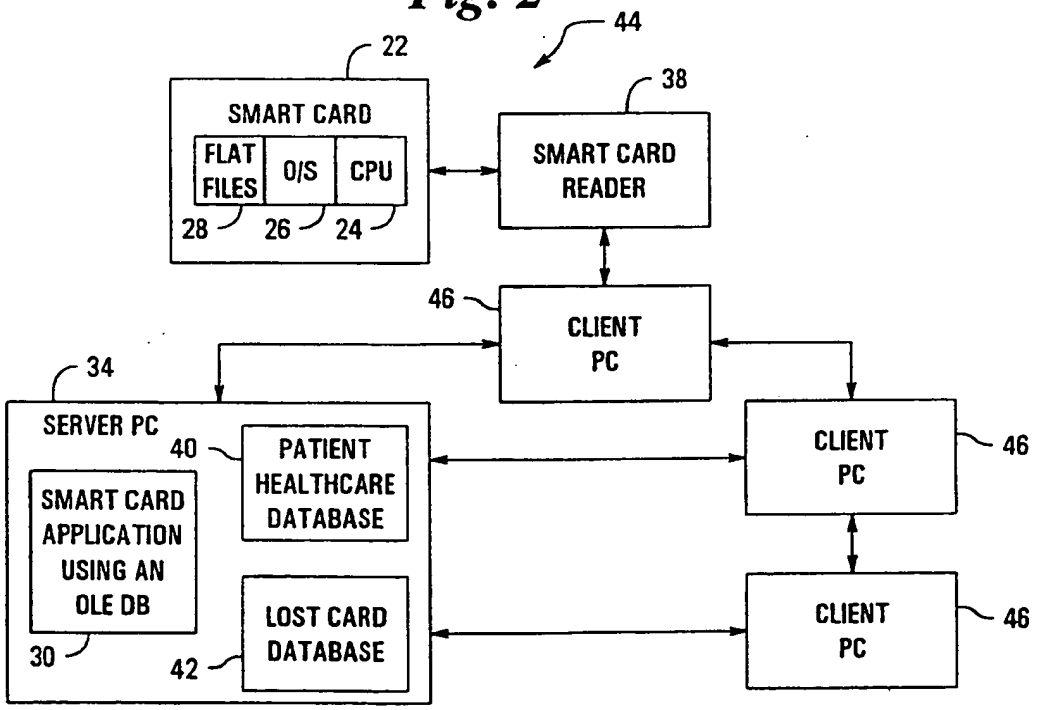

22
20
38
SMART CARD
FLAT FILES
O/S
CPU
28
26
24
SMART CARD READER
32
PC
40
PATIENT HEALTHCARE DATABASE
SMART CARD APPLICATION USING AN OLE DB
30
LOST CARD DATABASE
42

Fig. 2


44
22
38
SMART CARD
FLAT FILES
O/S
CPU
28
26
24
SMART CARD READER
46
CLIENT PC
34
SERVER PC
40
PATIENT HEALTHCARE DATABASE
SMART CARD APPLICATION USING AN OLE DB
30
LOST CARD DATABASE
42
CLIENT PC
46
CLIENT PC
46

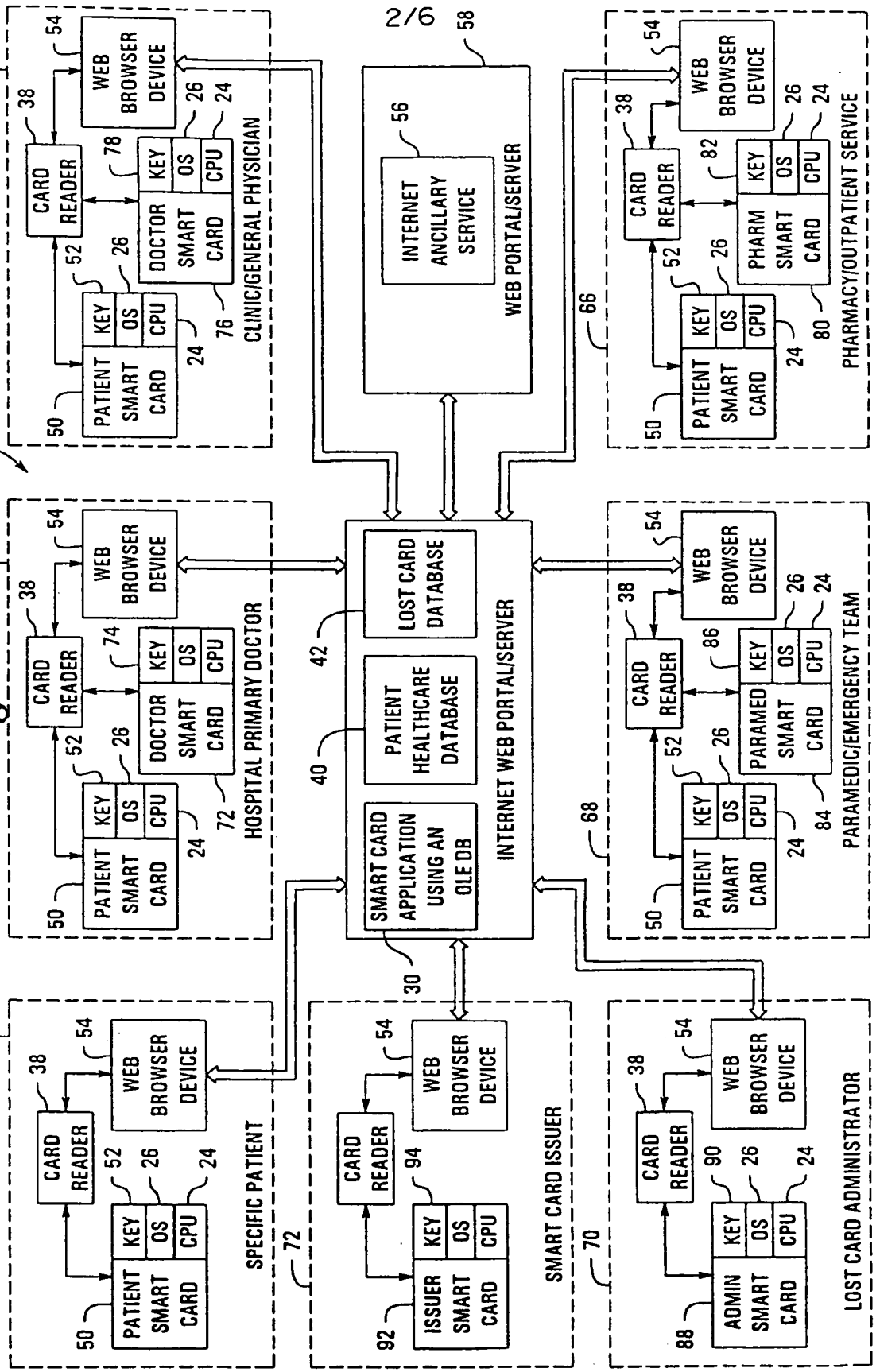

INTERNET WEB PORTAL/SERVER
LOST CARD DATABASE
PATIENT HEALTHCARE DATABASE
SMART CARD APPLICATION USING AN OLE DB
WEB PORTAL/SERVER
INTERNET ANCILLARY SERVICE
CLINIC/GENERAL PHYSICIAN
HOSPITAL PRIMARY DOCTOR
PHARMACY/OUTPATIENT SERVICE
PARAMEDIC/EMERGENCY TEAM
SPECIFIC PATIENT
SMART CARD ISSUER
LOST CARD ADMINISTRATOR
PATIENT SMART CARD
DOCTOR SMART CARD
PHARM SMART CARD
PARAMED SMART CARD
ISSUER SMART CARD
ADMIN SMART CARD
CARD READER
WEB BROWSER DEVICE
KEY
OS
CPU

Fig. 3

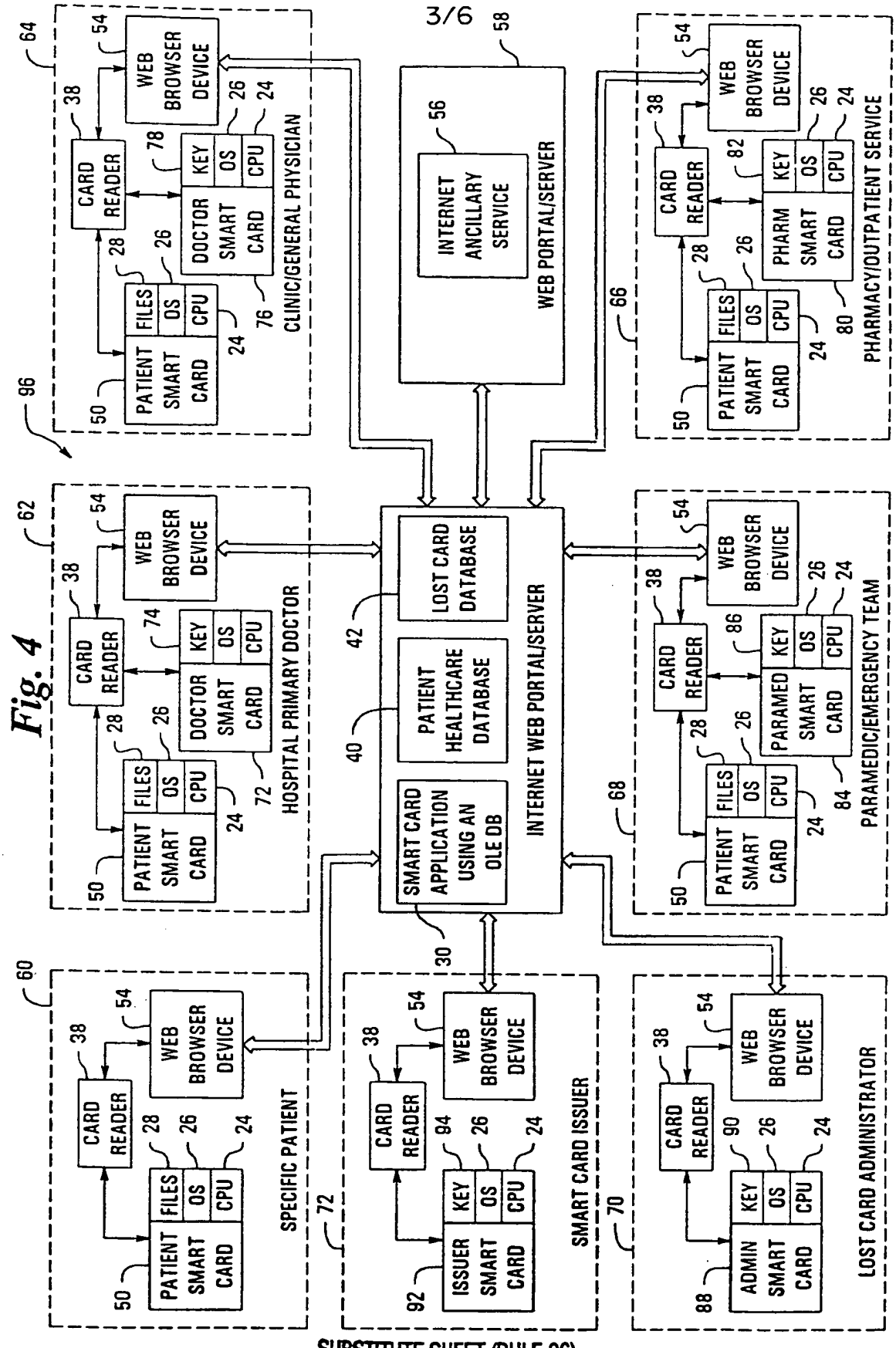

64
WEB BROWSER DEVICE
54
CARD READER
38
FILES
OS
CPU
PATIENT SMART CARD
DOCTOR SMART CARD
KEY
26
28
78
76
24
50
CLINIC/GENERAL PHYSICIAN
96
58
INTERNET ANCILLARY SERVICE
56
WEB PORTAL/SERVER
66
PHARM SMART CARD
82
80
PHARMACY/OUTPATIENT SERVICE
62
74
72
HOSPITAL PRIMARY DOCTOR
LOST CARD DATABASE
42
PATIENT HEALTHCARE DATABASE
40
SMART CARD APPLICATION USING AN OLE DB
INTERNET WEB PORTAL/SERVER
30
PARAMED SMART CARD
86
84
PARAMEDIC/EMERGENCY TEAM
68
60
SPECIFIC PATIENT
72
ISSUER SMART CARD
94
92
SMART CARD ISSUER
70
ADMIN SMART CARD
90
88
LOST CARD ADMINISTRATOR

Fig. 4

Fig. 5

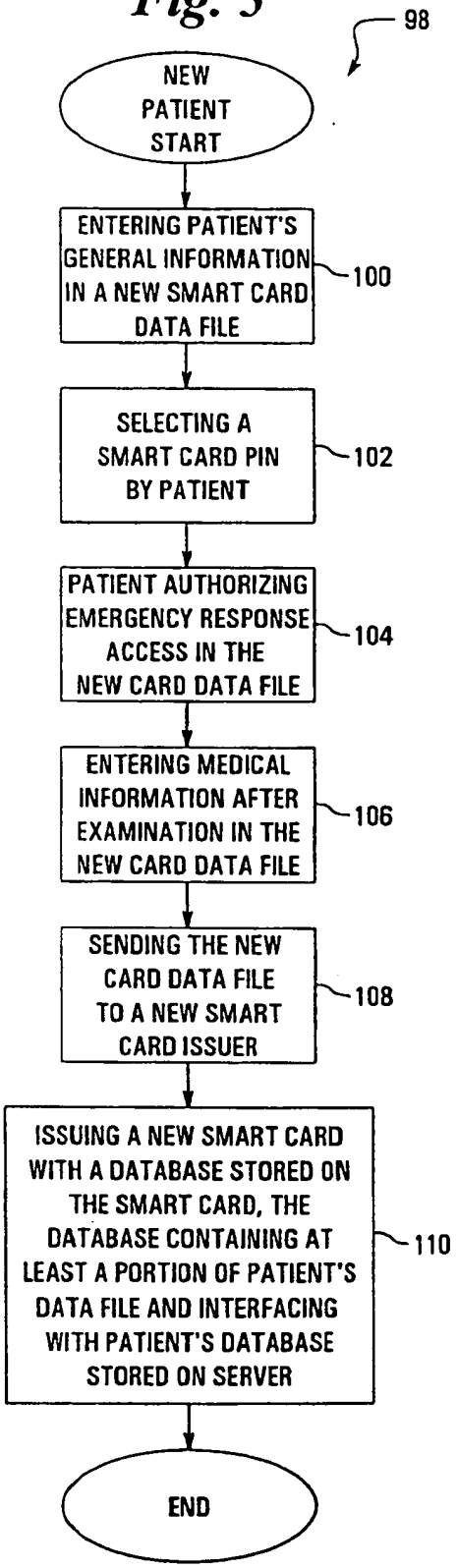

98
NEW PATIENT START
ENTERING PATIENT'S GENERAL INFORMATION IN A NEW SMART CARD DATA FILE
100
SELECTING A SMART CARD PIN BY PATIENT
102
PATIENT AUTHORIZING EMERGENCY RESPONSE ACCESS IN THE NEW CARD DATA FILE
104
ENTERING MEDICAL INFORMATION AFTER EXAMINATION IN THE NEW CARD DATA FILE
106
SENDING THE NEW CARD DATA FILE TO A NEW SMART CARD ISSUER
108
ISSUING A NEW SMART CARD WITH A DATABASE STORED ON THE SMART CARD, THE DATABASE CONTAINING AT LEAST A PORTION OF PATIENT'S DATA FILE AND INTERFACING WITH PATIENT'S DATABASE STORED ON SERVER
110
END

Fig. 6

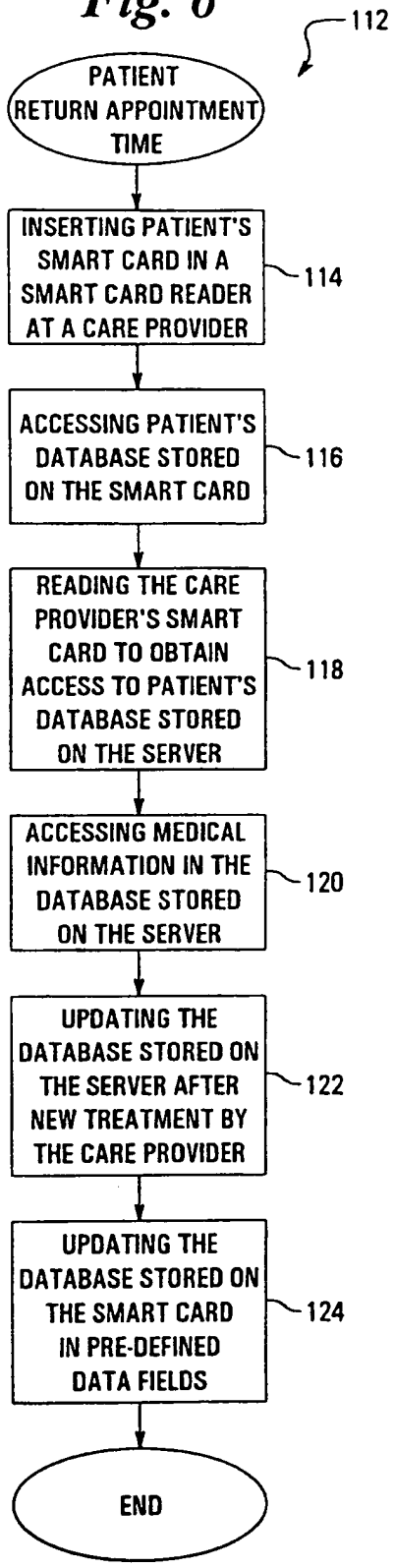

112
PATIENT RETURN APPOINTMENT TIME
INSERTING PATIENT'S SMART CARD IN A SMART CARD READER AT A CARE PROVIDER
114
ACCESSING PATIENT'S DATABASE STORED ON THE SMART CARD
116
READING THE CARE PROVIDER'S SMART CARD TO OBTAIN ACCESS TO PATIENT'S DATABASE STORED ON THE SERVER
118
ACCESSING MEDICAL INFORMATION IN THE DATABASE STORED ON THE SERVER
120
UPDATING THE DATABASE STORED ON THE SERVER AFTER NEW TREATMENT BY THE CARE PROVIDER
122
UPDATING THE DATABASE STORED ON THE SMART CARD IN PRE-DEFINED DATA FIELDS
124
END

Fig. 7

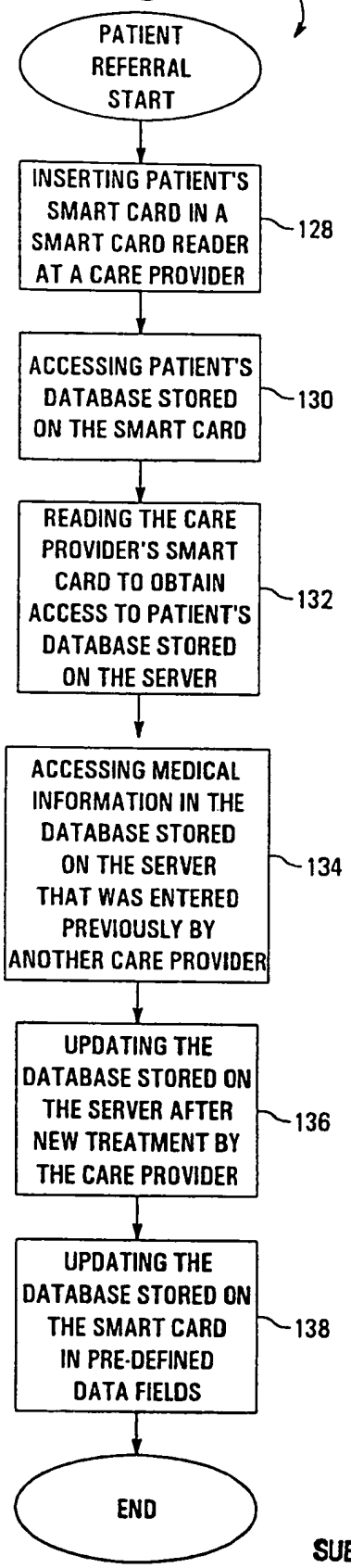

126
PATIENT REFERRAL START
INSERTING PATIENT'S SMART CARD IN A SMART CARD READER AT A CARE PROVIDER
128
ACCESSING PATIENT'S DATABASE STORED ON THE SMART CARD
130
READING THE CARE PROVIDER'S SMART CARD TO OBTAIN ACCESS TO PATIENT'S DATABASE STORED ON THE SERVER
132
ACCESSING MEDICAL INFORMATION IN THE DATABASE STORED ON THE SERVER THAT WAS ENTERED PREVIOUSLY BY ANOTHER CARE PROVIDER
134
UPDATING THE DATABASE STORED ON THE SERVER AFTER NEW TREATMENT BY THE CARE PROVIDER
136
UPDATING THE DATABASE STORED ON THE SMART CARD IN PRE-DEFINED DATA FIELDS
138
END

Fig. 8

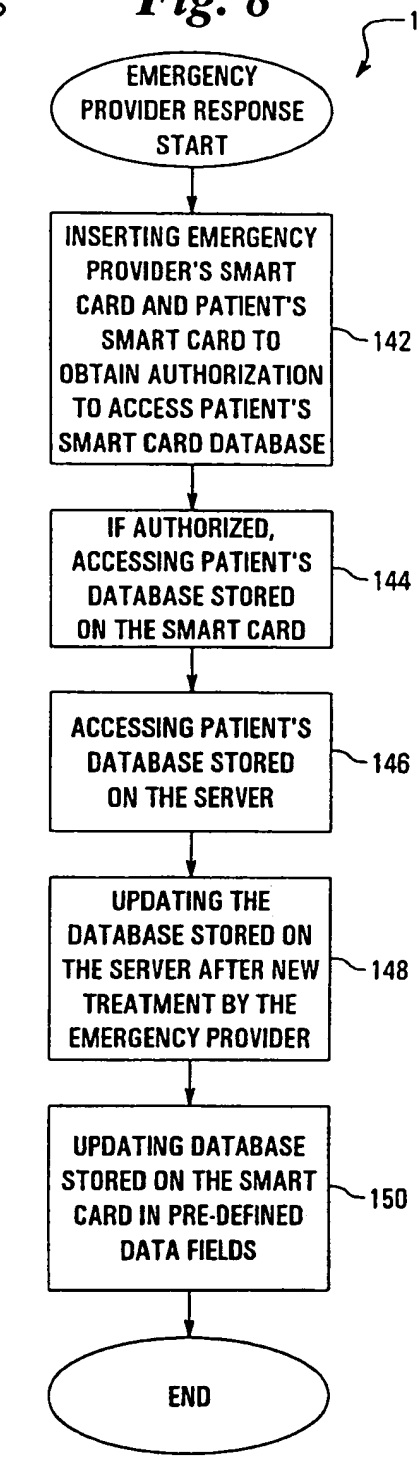

140
EMERGENCY PROVIDER RESPONSE START
INSERTING EMERGENCY PROVIDER'S SMART CARD AND PATIENT'S SMART CARD TO OBTAIN AUTHORIZATION TO ACCESS PATIENT'S SMART CARD DATABASE
142
IF AUTHORIZED, ACCESSING PATIENT'S DATABASE STORED ON THE SMART CARD
144
ACCESSING PATIENT'S DATABASE STORED ON THE SERVER
146
UPDATING THE DATABASE STORED ON THE SERVER AFTER NEW TREATMENT BY THE EMERGENCY PROVIDER
148
UPDATING DATABASE STORED ON THE SMART CARD IN PRE-DEFINED DATA FIELDS
150
END

Fig. 9

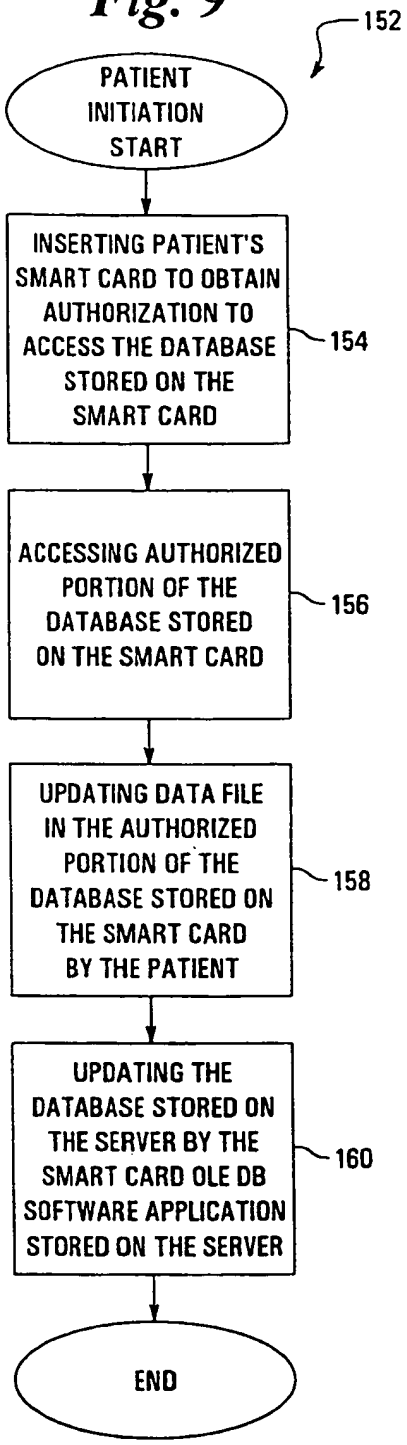
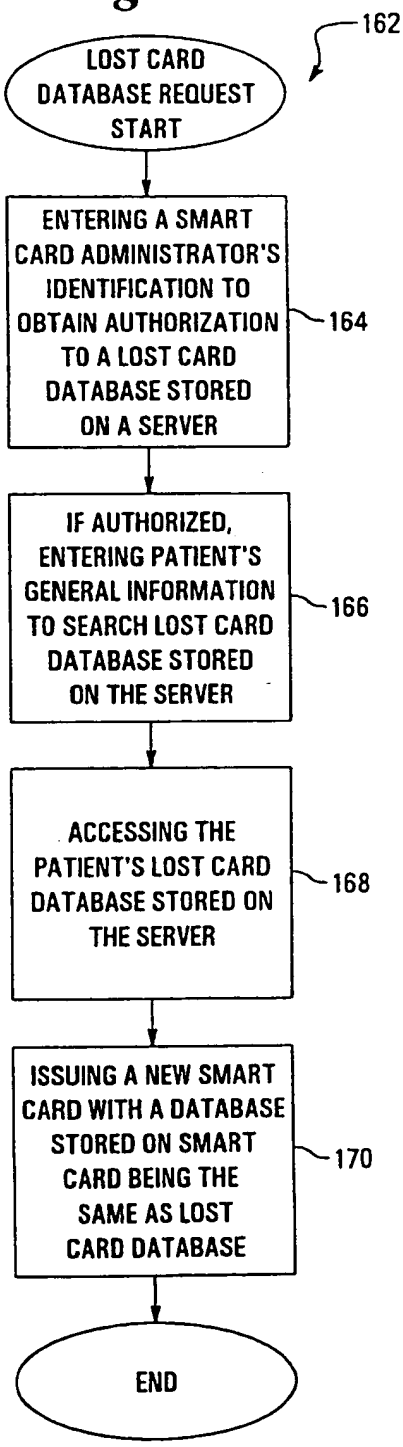

PATIENT INITIATION START
152
INSERTING PATIENT'S SMART CARD TO OBTAIN AUTHORIZATION TO ACCESS THE DATABASE STORED ON THE SMART CARD
154
ACCESSING AUTHORIZED PORTION OF THE DATABASE STORED ON THE SMART CARD
156
UPDATING DATA FILE IN THE AUTHORIZED PORTION OF THE DATABASE STORED ON THE SMART CARD BY THE PATIENT
158
UPDATING THE DATABASE STORED ON THE SERVER BY THE SMART CARD OLE DB SOFTWARE APPLICATION STORED ON THE SERVER
160
END

Fig. 10


LOST CARD DATABASE REQUEST START
162
ENTERING A SMART CARD ADMINISTRATOR'S IDENTIFICATION TO OBTAIN AUTHORIZATION TO A LOST CARD DATABASE STORED ON A SERVER
164
IF AUTHORIZED, ENTERING PATIENT'S GENERAL INFORMATION TO SEARCH LOST CARD DATABASE STORED ON THE SERVER
166
ACCESSING THE PATIENT'S LOST CARD DATABASE STORED ON THE SERVER
168
ISSUING A NEW SMART CARD WITH A DATABASE STORED ON SMART CARD BEING THE SAME AS LOST CARD DATABASE
170
END

INTERNATIONAL SEARCH REPORT

Inta Jonal Application No
PCT/US 00/19706

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F7/10 G06F19/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07F G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 0 764 911 A (EMX L.C.C.) 26 March 1997 (1997-03-26)	1,2,7,8, 11,12, 16,17, 22,25, 29,37, 40,43
A	the whole document	3-5,14, 23,26, 28,38, 41,44

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 December 2000	21/12/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	David, J

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Int. Jonal Application No
PCT/US 00/19706

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 97 22092 A (VENDA SECURITY CORPORATION) 19 June 1997 (1997-06-19)	1,2,7,8, 11,12, 16,17, 22,25, 29,37, 40,43
A	abstract; claims; figures	19,31, 33-36, 39,42, 45,46,48
A	EP 0 821 326 A (IBM) 28 January 1998 (1998-01-28) abstract; claims; figures column 6, line 11 - line 17	1-50
A	WO 97 04712 A (MC MEDICAL CARD SYSTEMS) 13 February 1997 (1997-02-13) abstract; claims; figure	1-50
A	US 5 291 399 A (J. CHACO) 1 March 1994 (1994-03-01)	
A	WO 96 08755 A (I. ROST) 21 March 1996 (1996-03-21)	

1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inte ional Application No
PCT/US 00/19706

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0764911 A	26-03-1997	AU 6193396 A	27-02-1997
		BR 9604121 A	23-09-1997
		CA 2182755 A	23-02-1997
		JP 9218902 A	19-08-1997
WO 9722092 A	19-06-1997	NONE	
EP 0821326 A	28-01-1998	DE 19629856 A	29-01-1998
		JP 10198606 A	31-07-1998
		US 6031910 A	29-02-2000
WO 9704712 A	13-02-1997	DE 19536204 A	30-01-1997
US 5291399 A	01-03-1994	US 5594786 A	14-01-1997
		US 5822544 A	13-10-1998
		US 5689229 A	18-11-1997
		US 5465082 A	07-11-1995
WO 9608755 A	21-03-1996	AT 163235 T	15-02-1998
		AU 3606795 A	29-03-1996
		CA 2199934 A	21-03-1996
		DE 19580995 D	04-12-1997
		DE 59501456 D	19-03-1998
		EP 0781428 A	02-07-1997
		ES 2116107 T	01-07-1998
		JP 10505695 T	02-06-1998